IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

DENISE DAICHENDT and ADA "JUNE" ODELL, individually, and on behalf of all others similarly situated,	)	
Plaintiffs,	)	Case No. 22 CV 3318
v.	)	Judge Robert W. Gettleman
CVS PHARMACY, INC.,	)	
Defendant.	)	

MEMORANDUM OPINION & ORDER

Plaintiffs Denise Daichendt and Ada "June" Odell bring this putative class action complaint, individually and on behalf of all other similarly situated persons (collectively, "plaintiffs"), against defendant CVS Pharmacy, Inc. ("CVS" or "defendant"). Plaintiffs allege various violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, under sections 15(a)–(c). Defendant moves to dismiss the class action complaint for failure to state a claim under Rule 12(b)(6) (Doc. 7). Fed. R. Civ. Pro. 12(b)(6). For the reasons stated below, the court grants defendant's motion to dismiss and remands certain claims to state court.

BACKGROUND

According to plaintiffs, defendant "takes passport and ID photos using the KODAK Biometric ID Photo System, which automatically verifies [that the] photos meet all government requirements." Plaintiffs allege that KODAK advertises the KODAK Biometric ID Photo System ("the photo system") as a means to "[p]rofit from passport photos" because photos for official documents like passports must meet certain requirements, including limitations on photo size, image size within the frame, and facial expression. The photo system is useful because it

confirms that the photos meet the required criteria through an application called "KODAK Moments."

Plaintiffs allege that KODAK Moments works by scanning consumers' facial geometry, and that a CVS employee first takes the photo with a digital camera and then uses the photo system to scan the digital image for biometric identifiers. According to plaintiffs, the photo system performs a "scan of face geometry on the consumer's photo," "collect[ing], captur[ing], and/or or [sic] otherwise obtain[ing] consumers' Biometrics." After taking the photo, consumers receive a printout with their photo and another printout with a verification certificate, the "Certificate of Biometric Passport Photos." Plaintiffs allege that the verification certificate "confirms that a scan of facial geometry was performed to confirm that the photos meet the following criteria": (a) the image is the correct size; (b) proper width/height ratio; (c) correct head size; (d) correct position of the head in the photo; (e) the image is sufficiently bright; (f) the image has a sufficient color balance; (g) eyes are open; (h) eyes are looking straight ahead; (i) mouth is closed and not smiling; (j) eye glasses are not present or there is no glare; and (k) proper facial position.

Plaintiffs allege that defendant's use of the photo system at CVS stores violates BIPA. According to plaintiffs, CVS is a private entity that "collects and stores consumers' biometric identifiers and biometric information . . . without first obtaining written consent or providing the same consumers with data retention and destruction policies." Plaintiffs also allege that defendant unlawfully profits from the sale or commercial use of consumers' biometrics. The case was originally filed in the Circuit Court of Cook County, Illinois, and was removed to this court under 28 U.S.C. § 1441. Defendant disputes all claims and brings the instant motion to dismiss.

LEGAL STANDARD

"To survive a motion to dismiss, a complaint must allege sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). For a claim to have "facial plausibility," a plaintiff must plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. "[W]here the well-pleaded facts do not permit the court to infer more than the possibility of misconduct, the complaint has alleged—but has not shown—that the pleader is entitled to relief." Id. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." Id.

DISCUSSION

The Illinois legislature enacted BIPA to protect residents' privacy interests in their biometric data.[1] See Heard v. Becton, Dickinson & Co., 440 F. Supp. 3d 960, 963 (N.D. Ill. 2020), citing Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197, 1199 (2019). BIPA contemplates two types of biometric data: "biometric identifiers" and "biometric information." A "biometric identifier" is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. On the other hand, "biometric information" is "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10. The legislature expressly excludes certain types of information from the definition of "biometric information," including confidential and sensitive non-biometric information that can be used to identify an individual. 740 ILCS 14/10. Ultimately, courts view "biometric" data as "biology-based." See, e.g., Rivera

[1] Courts analogize an individual's privacy interest in her unique biometric data to her interest in protecting her private domain from invasion, such as from trespass. See Bryant v. Compass Group USA, Inc., 958 F.3d 617, 624 (7th Cir. 2020), as amended on denial of reh'g and reh'g en banc, (June 30, 2020) and opinion amended on denial of reh'g en banc, 2020 WL 6534581 (7th Cir. 2020).

v. Google Inc., 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017).

Any person "aggrieved" by a violation of BIPA "shall have a right of action against an offending party," 740 ILCS 14/20, and plaintiffs claim that they were aggrieved by defendant's violations of three distinct sections: sections 15(a), 15(b), and 15(c). 740 ILCS 14/15(a)–(c). Section 15(a) requires that entities "in possession of" biometric data develop a publicly available retention schedule and destruction deadline for that data. 740 ILCS 14/15(a). Section 15(b) requires that entities collecting biometric data first inform the subject in writing that they are doing so, as well as state the specific purpose for its collection, storage, and use, and the length of time that they will store it. 740 ILCS 14/15(b)(1)–(2). Section 15(b) also requires that entities collecting biometric data receive written authorization. 740 ILCS 14/15(b)(3). Last, section 15(c) prohibits entities "in possession" of biometric data from selling, leasing, trading, or otherwise profiting from that data. 740 ILC 14/15(c).

Defendant moves to dismiss the class action complaint because it argues that plaintiffs fail to plead sufficient factual allegations to support their claims. First, defendant argues that plaintiffs do not sufficiently allege that defendant gained "control" over their biometric data pursuant to § 15(b) and provide only conclusory allegations regarding the verification certificate. Next, defendant argues that plaintiffs fail to sufficiently allege both "possession" and failure to comply under § 15(a). Last, defendant argues that plaintiffs fail to sufficiently allege both "possession" and "otherwise profit" under § 15(c).

The court evaluates each argument in turn but begins by remanding plaintiffs' claims under §§ 15(a) and 15(c) to state court based on lack of standing. The parties do not raise the issue of standing. Rather, the court raises this issue sua sponte, as it must. See, e.g., Cothron v. White Castle System, Inc., 467 F. Supp. 3d 604, 611 (N.D. Ill. 2020) ("Even when the parties do

not raise the issue of subject-matter jurisdiction, the Court must satisfy itself that jurisdiction is secure.") (internal quotations omitted). To establish standing in federal court, a plaintiff must allege an injury in fact, which must be actual or imminent, concrete and particularized, or else face dismissal. See Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992). Remand, not dismissal, is appropriate in the instant case because plaintiffs originally brought their claims in Illinois state court and standing requirements in Illinois courts are more lenient than the requirements for federal courts under Article III. See id. at 620.

The court first evaluates plaintiffs' claims under § 15(a). Defendant starts by arguing that the court should dismiss plaintiffs' claims under § 15(a) because plaintiffs fail to sufficiently allege that defendant "possessed" their data. Instead, defendant argues that plaintiffs rely solely on bald, parroted statutory language to trigger § 15(a) and allege that defendant "controlled" their biometric data. Next, defendant argues that plaintiffs conclusorily allege that defendant failed to comply with § 15(a) because defendant neglected to "maintain" a retention and destruction policy.

The court does not consider either party's arguments on the merits because it concludes that plaintiffs allege a bare procedural violation of § 15(a), and bare procedural claims are insufficiently concrete to establish standing in federal court.[2] See Bryant v. Compass Group USA, Inc., 958 F.3d 617, 626 (7th Cir. 2020), as amended on denial of reh'g and reh'g en banc, (June 30, 2020) and opinion amended on denial of reh'g en banc, 2020 WL 6534581 (7th Cir. 2020). The Seventh Circuit has held that a private entity's failure to create a retention and destruction policy alone is a bare procedural violation under § 15(a). See, e.g., Fox v. Dakkota

[2] Courts have explained that bare procedural violations of § 15(a) are violations of a general duty to the public, rather than concrete and particularized injuries, making them insufficient to establish Article III standing. See, e.g., Kislov v. Am. Airlines, Inc., 566 F. Supp. 3d 909, 914 (N.D. Ill. 2021).

Integrated Sys., LLC, 980 F.3d 1146, 1154–55 (7th Cir. 2020); Bryant, 958 F.3d at 626. On the other hand, a private entity's failure to comply with its policy may be sufficiently concrete to establish standing. See Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146, 1154–55 (7th Cir. 2020); Bryant, 958 F.3d at 626.

In the instant case, the court finds that plaintiffs have not alleged that defendant failed to comply with its retention and destruction policy and instead complain that defendant failed to "maintain" a retention policy to begin with. As the Seventh Circuit has clarified, failure to "create" a policy under § 15(a) violates § 15(a), but it is failure to comply with this policy, not failure to comply with § 15(a), that establishes standing in federal court. The court remands plaintiffs' claims to the extent that they allege a violation of § 15(a) without alleging a failure to comply with defendant's (allegedly nonexistent) retention and destruction policy.

Next, the court considers defendant's claims under § 15(c), which the court also remands to state court. Defendant argues that the court should dismiss plaintiffs' claims under § 15(c) because plaintiffs fail to sufficiently allege that defendant gained "possession" of their biometric data, and that defendant used their biometric data to "otherwise profit." The court cannot consider either argument because it finds that plaintiffs lack standing to bring their § 15(c) claim in federal court.

The court's reasoning in Hazlitt v. Apple, Inc., 543 F. Supp. 3d 643 (S.D. Ill. June 14, 2021), is instructive. In Hazlitt, the court remanded the plaintiffs' § 15(c) claim for lack of standing. Id. at 652. The Hazlitt plaintiffs alleged that the defendant violated § 15(c) because it used facial recognition technology to market and sell its devices and software, allowing it to "competitively position its devices and software in the marketplace, compete with other software applications, and thereby profit." Id. at 651. The court found that such an allegation did not

suggest that the defendant "sold or otherwise profited from their individual biometric data." Id. Without more, the court determined that plaintiffs did not allege a particularized harm as required by Article III. Id.

This court concludes that plaintiffs' § 15(c) claim in the instant case is like the plaintiffs' § 15(c) claim in Hazlitt. Plaintiffs do not allege that defendant profited from their individual biometric data, or from the putative class's data. Instead, they allege that defendant's conduct violates § 15(c) because it generally advertised the photo system, with its alleged use of biometric information, in order to generally profit from passport photos. As in Hazlitt, the court finds that this conduct is insufficient to establish Article III standing under § 15(c). Therefore, whether plaintiffs properly allege that defendant shared or transferred access to biometric data in return for something of value is irrelevant.[3] Accordingly, the court remands this claim.

Thus, this court is left with plaintiffs' claims under § 15(b). According to defendant, the court should dismiss plaintiffs' claims under § 15(b) because plaintiffs do not meet their factual pleading burden, and the verification certificate does not change this conclusion. Defendant argues that plaintiffs do not allege that defendant collects or captures biometric information; according to defendant, "[n]owhere do Plaintiffs allege what happens to the purported scan of face geometry, where it is stored, or what CVS supposedly does with it." Defendant concludes that plaintiffs' allegations do not suggest that defendant gained control of their biometric data.

Before it considers defendant's pleading burden argument, however, the court considers defendant's threshold argument that "the Photo System does not do anything that implicates BIPA." Defendant contends that "for a biometric identifier or biometric information to trigger BIPA at all, it must be plausibly alleged to be associated with an individual's identity."

[3] The court acknowledges defendant's point that plaintiffs, in their response to defendant's motion, do not dispute its argument that their claims under § 15(c) should be dismissed.

(Emphasis in original). According to defendant, because plaintiffs do not allege that defendant "used" any biometric data to determine plaintiffs' identities, BIPA does not apply. Relatedly, defendant argues that BIPA protections are not triggered by information obtained from scans of photographs. While the court disagrees with defendant's latter argument, it agrees with defendant that, based on the pleadings, BIPA does not apply to defendant's conduct here.

With respect to whether information obtained from scans of photographs can trigger BIPA, the court is inclined to conclude that the answer is "yes," although the court does not need to decide either way in the instant case. In Sosa v. Onfido, Inc., No. 20-CV-4247, 2022 WL 1211506 (N.D. Ill. Apr. 25, 2022), the court found that a scan of face geometry, even if the scan is "derived from" a photograph, falls under BIPA as a "biometric identifier." Id. at *6–7. The court determined that scanning photographs to locate facial images and extract a "unique numerical representation of the shape or geometry of each facial image" constitutes a scan of face geometry. Id. at *7 (collecting cases). The court emphasized that the statute does not define "scan of face geometry," and "nothing in [BIPA] expressly excludes information derived from photographs from the definition of 'biometric identifiers.'" Id.

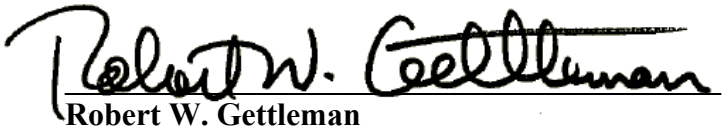
With respect to whether plaintiffs must allege that defendant "used" biometric data to determine their identities in order to trigger BIPA, the court agrees in part. The court disagrees with defendant that plaintiffs must specifically allege that defendant, in fact, "used" their biometric data to determine their identities. Instead, plaintiffs must allege that defendant's collection of their biometric data made defendant capable of determining their identities. See, e.g., Wise v. Ring, LLC, No. C20-1298-JCC, 2022 WL 3083068, at *3 (W.D. Wash. Aug. 3, 2022) (emphasizing whether the plaintiffs sufficiently alleged that the defendant "ha[d] the capacity to identify" the subjects of their face templates in evaluating the defendant's motion to

dismiss). The problem for plaintiffs is that their complaint contains no specific factual allegations to meet either burden. As defendant notes, plaintiffs do not plead that defendant, in fact, "used" their biometric data to determine their identities.[4] They also do not plead that defendant could do so. Plaintiffs do not allege that they provided defendant with any information, such as their names or physical or email addresses, that could connect the voluntary scans of face geometry with their identities. Thus, plaintiffs have failed to plead the most foundational aspect of a BIPA claim. Consequently, the court grants defendant's motion to dismiss plaintiffs' claims under § 15(b).

CONCLUSION

For the reasons stated above, defendant's motion to dismiss (Doc. 7) is granted. The court dismisses plaintiffs' claim under § 15(b) and remands plaintiffs' claims under §§ 15(a) and (c) without ruling on the merits. The Clerk is directed to remand this case to o the Circuit Court of Cook County, Illinois, forthwith.

ENTER:



Robert W. Gettleman
United States District Judge

DATE: December 2, 2022

[4] Plaintiffs' assertion that they "alleged facts evidencing that CVS actually used this information, to match it against passport photo regulations," is irrelevant to the court's inquiry and argues past defendant's argument rather than countering it. (Emphasis in original).